SECTION J, ATTACHMENT 3

PERFORMANCE SPECIFICATION 0700

FOR

COMMAND, CONTROL, AND DISPLAY SUBSYSTEM

FOR THE

INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEM-IV (ICIDS-IV)

04 May 2007

TABLE OF CONTENTS

1. SCOPE.

This Performance Specification (PS) specifies the major component requirements for the Command, Control, and Display Subsystem (CCDS) of the Integrated Commercial Intrusion Detection System (ICIDS). It establishes the performance, interface requirements and test requirements for the ICIDS CCDS. The ICIDS major components are:

a. Primary Monitor Console (PMC)
b. Console Uninterruptible Power Supply (UPS),
c. Remote Area Data Collector (RADC), and
d. Remote Status Monitor (RSM) with UPS.

External interface requirements to sensors, sensor stimuli, response devices, deterrent devices, Closed-Circuit Television (CCTV), Entry Control Equipment (ECE), Radio Frequency/Microwave and Fiber Optic Communication networks are specified herein. Performance requirements for the sensors, CCTV, and ECE are described in separate documents.

The CCDS configuration depends on the site size and the required security level. Figure 1 depicts typical ICIDS components used in an ICIDS configuration.

2. APPLICABLE DOCUMENTS.

2.1 Government Documents.

2.1.1 Specifications, Standards, and Handbooks.

The following documents, of the issue in effect on the date of the request for proposal, form a part of this PS to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the Department of Defense Index of Specifications and Standards (DODISS) and supplement thereto. In the event of a conflict between the text of this document and the references cited herein, the text of this specification takes precedence.

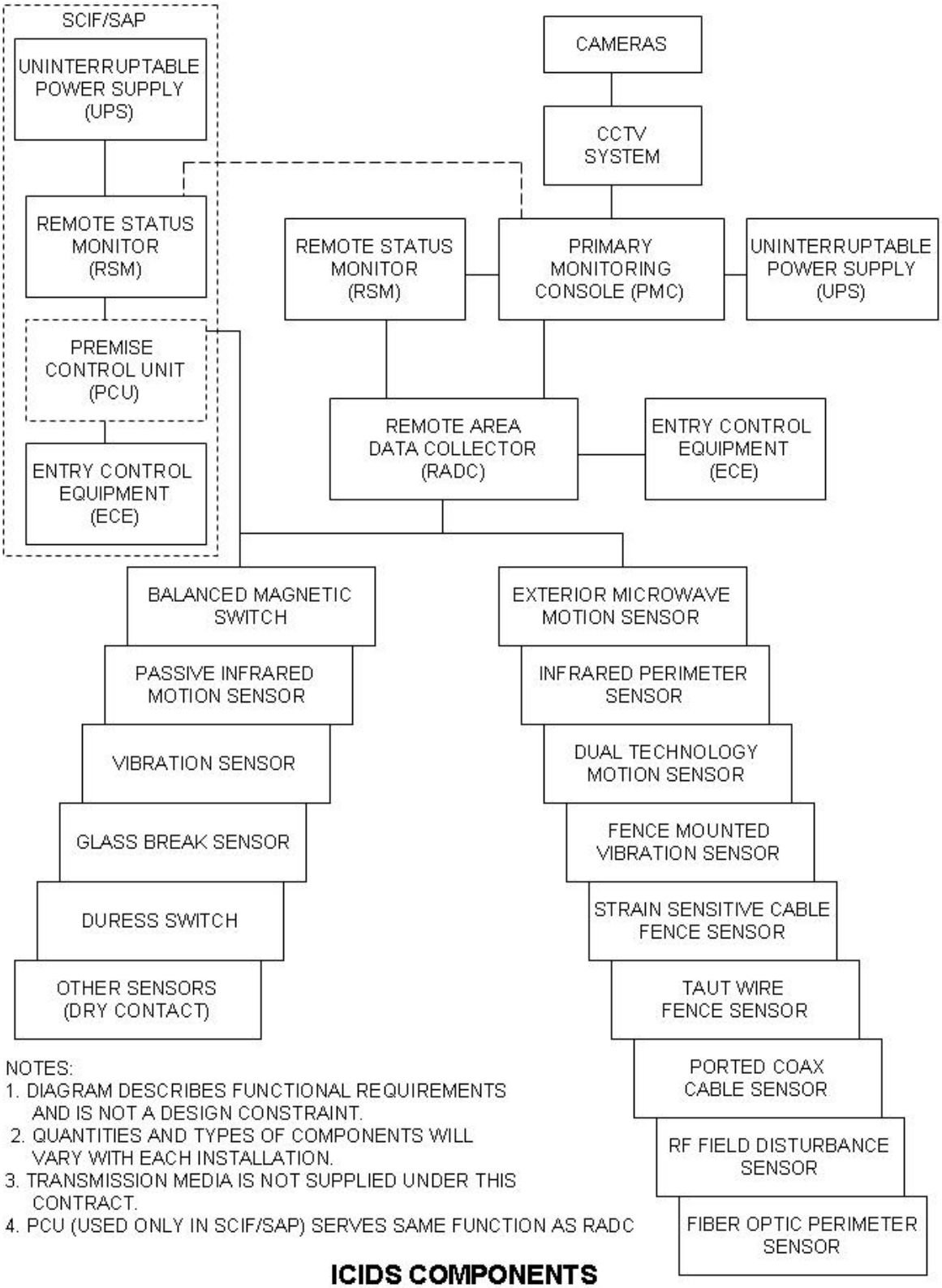
SCIF/SAP
UNINTERRUPTABLE POWER SUPPLY (UPS)
REMOTE STATUS MONITOR (RSM)
PREMISE CONTROL UNIT (PCU)
ENTRY CONTROL EQUIPMENT (ECE)
CAMERAS
CCTV SYSTEM
REMOTE STATUS MONITOR (RSM)
PRIMARY MONITORING CONSOLE (PMC)
UNINTERRUPTABLE POWER SUPPLY (UPS)
REMOTE AREA DATA COLLECTOR (RADC)
ENTRY CONTROL EQUIPMENT (ECE)
BALANCED MAGNETIC SWITCH
PASSIVE INFRARED MOTION SENSOR
VIBRATION SENSOR
GLASS BREAK SENSOR
DURESS SWITCH
OTHER SENSORS (DRY CONTACT)
EXTERIOR MICROWAVE MOTION SENSOR
INFRARED PERIMETER SENSOR
DUAL TECHNOLOGY MOTION SENSOR
FENCE MOUNTED VIBRATION SENSOR
STRAIN SENSITIVE CABLE FENCE SENSOR
TAUT WIRE FENCE SENSOR
PORTED COAX CABLE SENSOR
RF FIELD DISTURBANCE SENSOR
FIBER OPTIC PERIMETER SENSOR
NOTES:
1. DIAGRAM DESCRIBES FUNCTIONAL REQUIREMENTS AND IS NOT A DESIGN CONSTRAINT.
2. QUANTITIES AND TYPES OF COMPONENTS WILL VARY WITH EACH INSTALLATION.
3. TRANSMISSION MEDIA IS NOT SUPPLIED UNDER THIS CONTRACT.
4. PCU (USED ONLY IN SCIF/SAP) SERVES SAME FUNCTION AS RADC
ICIDS COMPONENTS

FIGURE 1

SPECIFICATIONS

FEDERAL

FCC Part 15	08 December 2003	Federal Communications Commission (FCC) Rules and Regulations

Department of Defense (DoD)

DoD C 5210.41-M	31 March 1983	Nuclear Weapon Security Manual

US ARMY

DA Form 4930-R	30 September 1980	Alarm/Intrusion Detection Record
AR 190-11	12 February 1998	Physical Security of Arms, Ammunition, and Explosives
AR 190-13	30 September 1993	The Army Physical Security Program
AR 380-381	21 April 2004	Special Access Programs (SAPS) and Sensitive Activities
AR 190-59	11 September 2006	Chemical Agent Security Program
UFGS 27 21 10.00 10	July 2006	Fiber Optic Data Transmission System
ICIDS-PS-0701	04 May 2007	Performance Specification for Closed Circuit Television Assessment Equipment of the Integrated Commercial Intrusion Detection System
ICIDS-PS-0702	04 May 2007	Performance Specification for Entry Control Equipment of the Integrated Commercial

		Intrusion Detection System
Numbered PES	12 January 2007	Performance Equivalence Sheets for ICIDS-IV provide minimum performance characteristics for interior and exterior sensors

STANDARDS

FEDERAL

Federal information processing standard publications:

FIPS 197	26 November 2001	Advanced Encryption Standard (AES)
FIPS 140-2	25 May 2001	Security Requirements for Cryptographic Modules

These documents can be found at the following web address: http://csrc.nist.gov/publications/fips/index.html

2.1.2 Other Government Documents, Drawings and Publications.

The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise indicated, the issues are those in effect on the date of the solicitation.

Director of Central Intelligence Directives (DCID):

DCID 6/9	18 November 2002	Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)

(Copies are available at the Program Office [PM-FPS] for review).

Joint Air Force, Army, and Navy Documents:

JAFAN 6/9	23 March 2004	Joint Air Force-Army-Navy Physical Security Standards for Special Access Program Facilities
DAMI-CDS Memorandum	01 March 2004	Updated Guidance for Installation of ICIDS in Army Sensitive Compartmented Information Facilities (SCIFs)

Army Corps of Engineers Guide Specification:

UFGS 27 21 10.00 10	July 2006	Fiber Optics Data Transmission Systems

(Guide Specifications may be accessed through the U.S. Army Corps of Engineers web site at:http://www.wbdg.org/ccb/browse_org.php?o=70)

Training and Doctrine Command Documents:

ICIDS Operational Requirements Document (ORD) 04 October 1994

Integrated Commercial Intrusion Detection System (ICIDS):

ICIDS	22 July 2005	ICIDS Security Classification Guide

2.2 Non-Government Publications.

The following documents form a part of this PS to the extent specified herein. Unless otherwise specified, the issues in effect on the date of the invitation for bids or request for proposal shall apply.

Underwriters Laboratories (UL) Standards:

UL 634	23 February 2000	Connectors and Switches for Use with Burglar-Alarm Systems, 8th Ed.
UL 639	21 February 1997	Intrusion-Detection Units, 7th Ed.
UL 1076	21 March 2005	Proprietary Burglar

Alarm Units and Systems.

(Application for copies should be addressed to Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062.)

National Electrical Manufacturers Association (NEMA):

NEMA 250-2003		Enclosure for Electrical Equipment (1000 v max).

(Application for copies should be addressed to National Electrical Manufacturers Association, 2101 L Street NW, Suite 300, Washington DC 20037.)

National Fire Protection Association (NFPA)

NFPA 70	2005	National Electrical Code.
NFPA 101	2006	Life Safety Code

(Applications for copies should be addressed to the National Fire Protection Association, International, 60 Batterymarch Street, Boston, MA 02110.)

(Non-government standards and other publications are normally available from the organizations which prepare or which distribute the documents. These documents may also be available in or through libraries or other informational services.)

2.3 Order of Precedence.

In the event of a conflict between the text of this PS and the references cited herein, the text of this PS shall take precedence. Nothing in this specification, however, shall supersede applicable laws and regulations unless a specific exemption has been obtained.

3. REQUIREMENTS.

3.1 Description.

The system consists of equipment in the monitor functional area, communications functional area, and remote functional area. The CCDS configuration described herein is

intended to illustrate functional requirements only and is not intended as a design constraint. All system components fall into one or more of these functional areas.

a. The monitor functional area equipment, through sequential polling, receives, processes, and displays remote area and system data. It executes command and control functions either automatically or under operator control. The monitor functional area equipment shall employ Open System Architecture.

b. The communications functional area equipment spans the distance from the monitor area to the remote areas.

c. The remote functional area equipment generates alarm and status change signals in response to local phenomena and collects and transmits this data. Selected remote area equipment also receives operator-commanded actions and executes operator-commanded actions.

The CCDS components shall each provide methods of self-protection, either individual or distributed. This protection shall include methods of component tamper security and inter-component communication link tamper security. System component design shall incorporate means of protecting the integrity of all communication links (e.g., line supervision, encryption).

All communication, power, and other interface lines shall be provided with Electromagnetic Interference (EMI), transient voltage, and surge protection, in accordance with paragraph 3.11, to prevent damage to equipment from lightning and other conducted electrical disturbances, or to localize damage in easily repairable low-cost components.

3.1.1 Major Component Groups.

The system contains:

a. Primary Monitor Console (PMC) capable of communicating over Government supplied communications media, including metallic wire pairs.

b. Remote Area Data Collectors (RADCs) capable of communicating over Government supplied communications media, including metallic wire pairs.

3.1.2 Other Components.

The CCDS may include any or all components specified herein, and shall interface and perform with the following components, as required, to form a complete ICIDS:

a. Remote Status Monitors (RSM) (see paragraph 3.4.2.3)

b. Sensors (see PES)

c. Data Authentication System (DAS) (see paragraph 3.5 herein)

d. Automated Entry Control Equipment (ECE) (see ICIDS-PS-0702)

e. Closed Circuit Television (CCTV) system (ICIDS-PS-0701)

f. Radio Frequency (RF)/Microwave Communication Link (see paragraph 3.6 herein)

g. Fiber optic communication interface (fiber optic cable is provided by the installation site) (see paragraph 3.7 herein)

h. Uninterruptible Power Supply (UPS) (see paragraph 3.4.2.1.10)

3.1.3 System Configurations.

The CCDS shall provide for expansion and flexibility of application to adapt to individual site characteristics. The interface and functional requirements, specified herein, apply to all CCDS, except as explicitly noted herein.

For the purposes of this PS, the two site characteristics which impact CCDS functionality and configuration are site size and security level. The system diagram, shown in Figure 1, depicts the configurations that conform to the requirements for each of the four security levels

and accommodates several user options (e.g., DAS, ECE, RADCs, and CCTV).

The four levels of security depend upon the assets being secured. The system configuration of Figure 1 and the applicable military requirements collectively define the equipment necessary to secure sites of all four security levels IAW AR 190-13, Chapter 4.

3.2 Construction.

The CCDS Construction shall meet the conditions specified in UL 1076, Sections 5 through 9.

3.3 Reliability and Maintainability.

3.3.1 Logistics and Readiness Requirements.

The ICIDS shall have a system operational availability (Ao) of 0.997 or greater, a mean time to repair (MTTR) of 0.5 hours, a maximum time to repair (MAX TTR) of 1.0 hours, a direct support maintenance ratio (MR) of 0.16 for the PMC and a service life of not less than 10 years. The initial mean time between operational mission failure (MTBOMF) for the display subsystem shall be 4,100 hours, a mean time between failure (MTBF) for any single transmission line of 21,400 hours, an MTBF for the RADC of 11,100 hours, and an MTBF for any sensor of 18,100 hours. Logistics and maintenance support will be accomplished by turn key contract or local contractual agreements at the installation level. The ICIDS integrated logistics support (ILS) plan will be tested during the initial operational test and evaluation of the system.

3.3.2 Failure Definition.

Failure is defined as any malfunction that results in loss of the ability of the equipment to perform its intended function.

3.3.3 Maintainability Characteristics.

The CCDS components shall incorporate features that enable cost effective maintenance throughout their deployed life. CCDS component maintainability features include:

a. Equipment shall remain operational during maintenance with all maintenance access covers, plates, doors, etc., removed or opened.

b. All indicators, which operator and maintenance personnel normally replace, shall be readily accessible.

c. Protective covers shall be installed over external connectors on remote area equipment with all-weather enclosures to prevent inadvertent damage or contamination.

d. Sized and keyed electrical connectors, plug-in assemblies, and controlled cable length shall be used to preclude mating to wrong receptacles.

e. Cable connectors and receptacles shall be marked with unique numerical designations to facilitate inspection and assembly. Labels and warnings shall be visible when the component is assembled.

3.3.4 Preventive Maintenance.

System components shall require minimal preventive maintenance. Provisions to perform preventive maintenance, while the system is operational, shall be provided.

3.3.5 System Endurance.

The system shall be capable of continuous operation (24 hours per day, 365 days per year) for the life expectancy of ten (10) years (minimum) with proper corrective and preventive maintenance.

3.3.6 Fault Detection/Fault Isolation (FD/FI).

FD/FI shall be incorporated to determine faults to the Line Replaceable Unit (LRU) (see 6.4.1).

3.4 Command, Control, and Display Subsystem (CCDS) Performance Characteristics.

3.4.1 General System Requirements.

3.4.1.1 To Report.

The CCDS installed in any ICIDS site, operated and maintained in accordance with established procedures, shall report detection of intruders, tampering, and equipment malfunctions. All detection information shall be processed and displayed to the operator of the system. Allow a duress alarm to

be output by the entering of a special code into a key pad or by activating a panic switch. Display the duress alarm at the network controller and operator console, but provide no indication of duress alarm at the local controller or key pad.

3.4.1.2 To Assess.

The system shall permit the operator to assess the nature of the intrusion via assessment devices, such as CCTV. The system design shall allow for automatic and manual control of assessment devices at the user's option. The operator shall not be able to manually activate the video assessment devices unless the remote area is in the Secure mode of operation or an alarm is present.

3.4.1.3 To Deter.

The system shall provide expandability to control four devices that deter or delay accomplishment of intrusion into protected area. The system design shall allow for manual operation of the response devices. The operator shall not be able to manually activate the response devices unless the remote area is in the Secure mode of operation and an alarm is present. The system design shall be robust enough to support controls that can provide on/off switches, Pan Tilt Zoom (PTZ) controls, or launch other autonomous devices.

3.4.1.4 System Timing.

The requirement for the system timing, via the RADC to PMC path, shall be any single alarm up to any five simultaneous alarms transmitted, processed and annunciated within a maximum total of 3.0 seconds after the alarms occurs.

a. If the RSM receives system status through the PMC, then the system timing via the PMC to RSM path shall be such that any single alarm is transmitted, processed and annunciated at the RSM within a maximum total of 2.0 seconds after display at the PMC. If the RSM communicates directly with the RADCs, then the system timing via the RADC to RSM path shall be such that any single alarm is transmitted, processed and annunciated within a maximum total of 3.0 seconds after the alarm occurs at the RADC. Neither RSM timing requirement shall increase the maximum PMC annunciation time.

b. The PMC shall interface to the CCTV switcher in a manner that requires the display of associated video within 1.0 second after the alarm is displayed.

3.4.1.5 Tamper Protection.

All CCDS components specified herein shall have tamper protection, unless otherwise specified. All removable panels, doors, drawers, or other access openings shall be equipped with tamper switches. The tamper switches on panels and doors shall be installed and baffled to prevent access, for defeating the switch, by deforming or opening the door or cover. The tamper switches shall be corrosion resistant to the environment to which they will be exposed. Tamper switches shall have maintenance positions that allow performance of maintenance tasks with the system fully operational. All doors shall be equipped with double action, high security locks. Information regarding approved locks shall be obtained from the Naval Facilities Engineering Service Center (NFESC), ATTN: Code ESC66, 1100 23rd Avenue, Port Hueneme, CA 93043-4370. The use of any master key system or multiple key system is prohibited.

3.4.1.6 Printer.

Multiple printers are permitted. The printer shall provide the following capabilities:

a. Event printing: The printer shall be capable of printing record all significant system activity (alarms, status changes, etc.) including date, time and all operator actions, whether displayed or not.

b. Log printing: The printer shall also have the capability to allow the operator, maintainer or supervisor, under key, password or other control, to print reports of historical system data selected from a number of pre-defined (ex. DA form 4930-R: Alarm/Intrusion Detection Report) or user-defined formats and contents.

3.4.2 CCDS Major Components.

3.4.2.1 Primary Monitor Console (PMC).

3.4.2.1.1 Description.

The PMC is a monitor area item and shall utilize an interrogate-response polling sequence to provide the primary command and control for the secure areas, hereafter called remote areas. The PMC shall have the capability to monitor up to at least 512 remote areas controlled by RADCs.

3.4.2.1.2 Functional Areas.

The major functional areas of the PMC are:

a. Command, Control, and Display (CCD),

b. operator interface including operator input devices, maintenance input devices, video status display, geographic and remote area graphic display, CCTV controls and monitors, and audible alarms and printer,

c. remote area communication,

d. interconsole communication (PMC to RSM[s]), and

e. system data storage.

3.4.2.1.3 Command, Control and Display Functions.

The Command, Control and Display functions shall be to:

a. Supervise all PMC, RADC, and RSM communications and data flow.

b. Communicate with the remote areas (RADCs) by way of pseudo-random generated tones or digital encoding using an interrogate and response protocol to determine the status of each remote area, and annunciate all status changes. Status changes include, but are not limited to, alarm, ACCESS/SECURE/OFF-LINE, and entry denied.

c. Provide the communication interfaces to connected RADCs and RSMs with the following capabilities:

(1) Send and receive data by one of the following separate data link interfaces and subsystems. The PMC is required to support any combination of the following data links, as selected by the user. The choice of data link shall be made by the user and shall not limit any system performance nor preclude the use of the DAS, whether internal or external:

(a) Interfaces with continuous metallic wire pairs are required for all data links of the PMC.

(b) A commercial RF/microwave data link may be specified, prior to installation, for some or all remote area or PMC-to-RSM communication links. It shall be compatible with the metallic wire pair interfaces at the PMC, RSM, and RADC.

(c) A commercial fiber optic communication interface is an option to be specified by the user for some or all remote area or PMC-to-RSM data communication links. The transmit/receive circuitry which interfaces to the fiber cable may be internal (e.g., replaces hardwired modem) or external (e.g., connects to PMC hardwired output). It shall be compatible with the PMC, RSM and RADC data communication interfaces. The fiber optic communication interface shall utilize fiber optic cable and components as specified in UFGS 27 21 10.00 10, Fiber Optic Data Transmission System for Security Systems.

(2) Execute error detection and line supervision processes in order to monitor, detect, and report the loss of line integrity of the communication links.

(3) The PMC-to-RADC and PMC-to-RSM links (as architecture dictates) shall be capable of operating up to 16 kilometers without repeaters or relays.

(4) Exchange information over the RADC interface including:

(a) Sensor alarms

(b) Sensor tamper

(c) RADC status including ACCESS/SECURE/OFF-LINE mode

(d) RADC tamper

(e) RADC power supply fail alarms

(f) Response device commands

(g) Response device status

(h) Remote area configuration

(i) Self-test commands and results

(j) Entry Control Equipment data (e.g., entry approved/denied). The PMC shall be notified of any shunted RADC or sensor.

(5) Exchange information over the RSM interface including all, or user-selected, portions of the system status. The user selects the information to be passed over this link at the time of initial system configuration, and it is a maintenance function to configure the PMC and/or RSM to implement these selections.

(6) Provide an interface for the optional use of the DAS with any or all of the communication links.

For ICIDS installations with SCIF remote areas, which are not located in areas within Government controlled facilities within CONUS, line supervision is required in accordance with the requirements identified in DCID 6/9.

For ICIDS installations with the PMC and RSM installed within a SCIF, line supervision is required in accordance with the requirements identified in DCID 6/9.

d. Monitor the tamper conditions for the PMC and PMC power supply.

e. Monitor AC power status for the PMC.

f. Monitor operator input device data, such as commands and requests.

g. Provide the capability to assign a priority level to each RADC. The PMC shall display alarms, according to this priority, regardless of the sequence of arrival. A minimum of four levels of priority are required. Alarms of the same priority shall be displayed in the sequence of arrival.

h. Support the RADC interface to Entry Control Equipment (ECE). The PMC shall receive and display entry control information including, but not limited to, entry approved, entry denied alarms, and tamper from the RADC. Functions required of the ECE may be implemented at either the PMC or RADC, but, in all cases, ECE data and processing shall be subordinated in priority to intrusion data and processing. The processing of ECE data at the PMC shall not affect the system timing requirements. Functional requirements for the ECE system are specified in ICIDS-PS-0702.

i. Provide an interface with a CCTV system that shall perform as described in 3.4.2.1.11. Functional requirements for the CCTV system are specified in ICIDS-PS-0701.

j. Automatically activate the video cameras, upon receipt of the first alarm from the remote areas, to enable operator assessment of remote area alarms from remote areas equipped with cameras. In the case of multiple alarms, means shall be provided to allow the operator to manually select the video for each subsequent alarm. New alarms, regardless of priority, shall not take precedence over alarms currently being addressed by the operator nor automatically change the status or geographic displays; the video for the new alarm(s) shall be activated only upon manual operator selection.

k. Provide an interface for a printer(s). The PMC shall print a hard copy of all system activity, including operator actions. The PMC shall also have the capability to allow the maintainer or supervisor, under key, password, or other control, to print reports of historical system data. When the printer is OFF-LINE or printing requested reports, data shall continue to be stored for retrieval when the printer is restored ON-LINE.

l. Print or display the system configuration data, including date and time, of the most recent system configuration changes.

m. Provide for orderly shutdown and restart whenever components are replaced or have lost information because of power failure or component failure.

n. Provide for automatic, nonvolatile data storage of historical data, system configuration data, and system status such as graphic maps, CCTV maps, configuration tables, databases, periods of maintenance, and sensor shunting. The operator shall have no control of data storage. Access to replacing, printing, or backing up the historical data shall be restricted to personnel with the appropriate level of access.

o. Have provisions for automatic storage of system configuration data and automatic reinitialization of system configuration from data storage after any system outage (i.e., power outage or system maintenance downtime). Reinitialization time from power on until full system operation shall not exceed five minutes.

p. Provide for both a manual and an automatic self-testing of the system with the capability for user definable and programmable parameters at installation. These parameters shall include duration of test, number of tests per a given time period, and other required system test parameters data. The interval between automatic tests shall be randomized. Annunciation of intentional alarms generated on a specific device, while under self-test, shall be suppressed. Any valid alarm such as intrusion, tamper or duress (other than an intentional alarm), generated during a self-test, shall cause the self-test to

terminate and the alarm shall be annunciated. The results of all self-tests shall be recorded on the printer and in the system data storage. Only self-test failures shall be annunciated at the PMC status displays. Any mode change from ACCESS to SECURE shall automatically initiate a self-test of the remote area equipment within 90 seconds after the mode change.

q. Provide for two processes to change the ACCESS/SECURE mode of operation of a RADC for an individual sensor or for the entire RADC: 1) from the PMC or RSM in CCD mode, or 2) from the RADC. The functional requirements of the ACCESS and SECURE modes are described herein and shall be implemented at the RADC regardless of the process used to change the mode.

   The operator shall have the capability to change the ACCESS/SECURE mode of a remote area or sensor by entering a command at the PMC (except for SCIF areas where remote commanded ACCESS/SECURE is prohibited or locked-out at installation). The two-person rule requirements shall apply to commanded ACCESS/SECURE mode changes when so configured at installation.

   Both of these operating mode changes shall be handled identically. The PMC shall monitor and continuously display the mode of operation of the sensors and RADCs. SECURE mode shall be indicated by green color for icons, indicators and graphics; ACCESS shall be indicated by yellow color,

r. Provide EMI, transient voltage, and surge protection on all external interface lines, in accordance with paragraph 3.11.

3.4.2.1.4 Operator Interface.

The PMC command and control devices shall provide an integrated operator interface and provide at least four levels of access to operator functions. Access to each level shall be regulated by passwords or other means such that an operator possessing the lowest level of access may perform the minimum functions necessary to operate the system, and the other functions may be individually allocated to any of the other access levels. The system shall be able to support at least 25 passwords, each assigned to an access level. An operator with a password assigned to one access level can use the functions

allocated to that and all lower levels, but shall not be able to use the functions allocated to any higher level. The system shall prepare a report presenting the available data required on DA Form 4930-R, Alarm Intrusion Detection Record. The report shall be populated by the available system data for each alarm reported via the alarm queue. This report shall provide space for the operator to add additional data that is not provided by the ICIDS system.

a. An operator input device (mouse, keyboard, or other) to implement the command, control, and display functions is required to issue commands. All operator functions shall be selected via dedicated or extensible function keys, mouse click, or other means. No operator actions shall require memorization of command strings and shall be tied to a minimum number of key-strokes (e.g., 1 or 2.). In addition, only one action (key stroke or mouse click) shall be required to acknowledge an alarm. The operator controls shall be clearly labeled as to their function. General purpose keyboards or specialized keyboards are permitted. The operator, with proper password, shall have the capability to selectively address the remote areas for such purposes as:

(1) Placing remote areas or specific individual sensors in ACCESS or SECURE mode (except as prohibited for SCIFs in paragraph 3.4.2.2.8). The user, at initial system configuration, assigns to each RADC either unrestricted or two-person rule requirements for the ACCESS\SECURE mode changes. The unrestricted assignment allows a single PMC operator to command mode changes without the need for concurrence.

The two-person rule assignment shall implement the DoD and service requirements specified herein. This capability shall be provided as a user option, selectable for specific remote areas or specific individual sensors at initial system configuration. When this option is selected, a single PMC or RSM operator shall be prohibited from commanding remote areas or individual

sensors OFF-LINE (e.g., for maintenance) or into ACCESS.

Two-person commanded ACCESS and commanded OFF-LINE from the PMC shall require cooperative action between two persons, either both at the PMC, or one person at the PMC and one person at the RSM, or both persons at the RSM (when in the CCD mode). When an operator commands (requests) a remote area or sensor into ACCESS or OFF-LINE, the second person (another operator, supervisor, or other authorized party) shall have means to concur with the command (acknowledge the request) within a reaction time period of 2 to 12 seconds (adjustable at initial system configuration) for the commanded action to take effect or be successfully completed.

In the absence of concurrence by the second operator before the reaction time, both audible and visual alarms at both consoles indicating a two-person rule violation shall be annunciated. The commanded action shall then be locked out and the violation alarms remain active until the operator, initially requesting the action, removes the request. Removal of the request shall automatically clear the alarm.

In the two-person rule process, the initial action is considered a request for the status or mode change. For the PMC or RSM initiating the action, the request is identical to the command or action used when two-person rule is not required. The concur action can take the form of a password entry, key switch or other dedicated process by a person other than the operator at the requesting PMC or RSM; or by a command key, password entry, or other action at the RSM. In all cases, the two-person rule design and implementation shall ensure the integrity and security of the intended process.

(2) Initiating a remote area sensor test and selectively initiating tests of system functions. This shall be in addition to periodic automatic testing.

(3) Activating response devices. The PMC shall provide the operator control to enable and disable, and activate or deactivate remotely controlled response devices. A response device must first be manually enabled by a PMC command before it can be manually activated. The PMC operator shall have the capability to activate a response device after correctly entering the activate command for the specific response device desired only when the RADC is in SECURE mode, the response device has been previously enabled, and an alarm is present.

(4) Acknowledging and resetting status changes. The operator shall be provided the capability to selectively acknowledge and reset alarms and status changes in order to return the system functions to their normal operating state. Acknowledging is defined as a PMC operator action using a single action to silence the audible alarm, and changes the displayed status of the event (alarm, AC power, etc.) from active (flashing red) to pending (steady red). A pending alarm is defined as an alarm that has been acknowledged (audio alarm silenced), but not reset. The graphic and status messages for a pending sensor alarm shall change to flashing red when the sensor re-alarms. All alarms and status changes shall be acknowledged before they can be reset. Resetting an alarm is defined as a PMC operator action (e.g., a keystroke), which changes the displayed status of the event from pending (steady red) to clear or reset (steady green) and returns the sensor or device to the ready state. The PMC shall not allow any active alarm to be reset. The ‘acknowledge’ and ‘reset’ functions shall be provided for operator selected groups of RADCs.

(5) Selectively display individual remote area status or the primary screen on the status display, and provide the capability for the operator to access additional display screens as required. The primary screen is that which is normally shown on the status display; it contains the alarm display and system summary information detailed in paragraph 3.4.2.1.7. Individual remote area status screens and additional (secondary) display screens shall contain such information as operator instructions, response force information, and details of the alarm zone. In the event of a new alarm, the display shall not automatically revert from secondary screens to the primary screen.

b. A maintenance input device (mouse, keyboard, or other) to permit a maintenance technician to perform required maintenance tasks. Unauthorized access to the maintenance input device shall be protected against by a mechanical and/or electrical lock (e.g., password, locked panel, etc.).

The PMC shall provide access to maintenance functions. Access shall be regulated by password or other means.

The PMC shall be capable of allowing all maintenance tasks except initial configuration to be accomplished while the PMC is on-line and fully operational. On-line maintenance shall not interfere with normal system operation nor cause the loss of any real-time or historical system data. The maintenance tasks shall include:

(1) Setting the time and date.

(2) Establishing, backing up, modifying, reloading (restoring) and recording (saving) the system configuration (database). All activities and parameters identified within this PS, which are established at initial system or device configuration, may also be

modified by maintainers with the proper access level while the PMC is on-line.

(3) Graphic display generation.

(4) System initialization and reinitialization.

(5) Setting self-test parameters.

(6) System self-diagnostics (shall be disabled for RADCs installed in SCIFs).

(7) Printing various reports of historical system activity from system data storage.

(8) Selecting the portion of the PMC display to be displayed at RSM (if accomplished at PMC).

c. A video status display, a primary source of system information for the operator. The performance requirements of the status display are specified herein.

d. The video geographic map display for use by the operator to assess alarm location within the remote area and geographically within the site to assist in dispatching response teams. This single display shall be used for both the remote area graphic display and the geographic map display.

e. CCTV controls and monitors for operator assessment for remote area alarms that allow automatic alarm-triggered and manual operator-triggered selection of any camera onto any of four monitors. A fifth monitor shall be used for viewing video storage system images.

f. Audible alarm (audible tone signals) for annunciation of all alarms and system status changes. A dedicated control shall be provided to adjust the auditory signal volume to be easily heard above any expected ambient noise. A control shall be provided (e.g., acknowledge key) that silences the audible alarm for the current event only (alarm, status change, etc.). The

audible alarm shall be activated for each new alarm. For repeated alarms, the audible alarm shall be reactivated to indicate any change in state of any alarm (e.g., from pending (acknowledged) to active (alarmed)).

g. A printer is required to provide a permanent record of all operator and system activity at the PMC, and as a secondary display for the operator in the event of a primary display failure. Multiple printers are not prohibited. The printer shall provide controls for the operator to put the printer ON-LINE/OFF-LINE for adding paper and clearing paper jams. When the printer is OFF-LINE, or printing requested reports, system activity shall continue being stored for later retrieval.

3.4.2.1.5 Remote Area Communication.

The PMC shall:

a. interface with system RADCs,

b. interface with collocated ECE, and

c. interface with a DAS to encrypt/decrypt all PMC-to-RADC data communication over that DAS data link. The DAS may be used on any or all PMC-to-RADC data links. Disruption or loss of this communication link shall be annunciated at the PMC and RSMs as a line security alarm. When communication is lost or tampered between RADCs and remote area devices (e.g., sensors), a tamper or other distinct alarm shall be displayed at the PMC and RSMs.

3.4.2.1.6 Interconsole Communication.

The PMC shall:

a. Communicate (directly, if architecture dictates) all or selected portions of the system status, and all PMC operator actions for use by the RSMs.

b. Interface with a DAS to encrypt system data for use by the RSMs. Disruption or loss of these communication lines shall be annunciated at the PMC and RSMs as line security alarms.

c. Provide system status data for use of up to 8 RSMs on links capable of operating up to 16 kilometers without repeaters or relays.

d. The PMC shall provide the capability, upon configuration at the user's option, to automatically assume control of all remote areas upon failure of the RSM in CCD mode; or, to automatically relinquish control to an RSM(s) in CCD mode upon failure of the PMC. Control shall be capable of being switched to and from the RSM, either manually or automatically (according to a schedule or due to failure of PMC or RSM); however, the switchover shall not disrupt the continuous monitoring of RADCs or cause loss of any system data.

3.4.2.1.7 Status Display.

The PMC shall provide a dedicated visual status display, in color, which provides all of the remote area and system status information. The display format shall provide for rapid operator comprehension. This shall include the use of color, blinking fields, highlights, and other techniques to draw attention to alarms and status changes. The PMC status display shall:

a. Continuously provide the operator with summary status information for the complete system including alarm data on a time, location and component basis. Components for which alarms must be reported in the system summary include sensors, sensor loops, RADCs, UPSs, communication lines, and any system component that reports or is monitored for alarm. Alarm types include intrusion, tamper, line security, communication fault/failure, input power status (AC/DC), and other alarm types. Other status messages include ACCESS/SECURE/OFF-LINE mode for RADCs and sensors, maintenance mode for RADCs, power source (AC/DC) for PMC and RADCs, shunted sensor(s), and other potential status messages.

b. Display alarms in prioritized order independent of the sequence of arrival at the PMC. Alarms of the same priority shall be displayed chronologically within that priority level (see also 3.4.2.1.3.g). Alarms shall remain displayed until reset. Automatic prioritization of alarms in at least four user-defined levels is required (i.e., any subsequent alarms must be automatically organized on the status display in the prioritized order without requiring operator action).

c. Display, upon command, the status of each individual sensor and response device.

d. Display each status change as it occurs.

e. Display any special instructions for actions to be taken. This message shall be input by the PMC maintainer during system configuration.

f. Provide response device status (e.g., armed, disarmed, fired, safe).

g. Echo all operator inputs.

h. Display entry denied alarms and other ECE data at a priority level subordinate to intrusion alarms.

i. Continuously display an indication for the duration each RADC is in maintenance mode. Continuously display all RADCs and sensors that have been shunted.

j. Contain text consisting of standard typewriter alphanumeric characters in upper and lower case. The text font and size shall produce an 80 column by 25 line display, and each character shall be displayed in any of 16 colors, selected by the user, except where previously defined in this performance specification.

k. Utilize a color visual display of at least 48 centimeters diagonal in size with a minimum resolution of 1280 X 1025 pixels.

3.4.2.1.8 Geographic Map Display.

The PMC shall provide a geographic map display that depicts each remote area by a representative map of the remote area, including surroundings. The geographic map display shall:

a. Provide a unique remote area graphic for each remote area to be created and edited by the user. Each graphic shall consist of text, symbols, lines and areas selected and placed by the user. The text shall consist of standard typewriter alphanumeric characters in upper and lower case. The text font and size shall produce an 80 column by 25 line display, and each character shall be displayed in any of 16 colors, selected by the user. The symbols shall consist of any custom symbols that expedite preparation and interpretation of the graphic. The symbols shall be displayed in the same size as the text in any of 16 user-selected colors. The lines shall consist of straight-line segments in any orientation, in either of two widths, single or double, and in any of 8 user-selected colors. The areas shall be definable in a consistent manner and be displayed in any of eight user-selectable colors.

b. Represent walls, doors, and miscellaneous objects on maps of the interior areas. Represent fences, gates, roads, and miscellaneous barriers and objects on maps of the interior areas.

c. Allow the user to depict the location of each sensor in the remote area using defined, unique, and easily identifiable graphic symbols. The display shall automatically depict the status of each sensor in the remote area using color coding of the sensor symbols as follows:

   - Steady green indicates SECURE operation (reset and no-alarm),
   - Steady yellow indicates ACCESS,
   - Flashing red indicates unacknowledged alarm,
   - Steady red indicates acknowledged alarms,
   - Steady gray indicates the sensor is shunted or masked.

d. Allow the user to depict the location of each response device in the remote area using defined, unique, and easily identifiable graphic symbols. The display shall automatically depict the status of each response device in the remote area using color coding of the symbols as follows:

- Green indicates SAFE,
- Steady Yellow indicates ARMED,
- Steady Red indicates FIRED.

e. Automatically display the map of remote area in alarm, upon receipt of an alarm in that area, or upon operator request.

f. Provide storage media interface and functions that permit the duplication of all remote area graphics to removable media for backup and secure storage, and permit the regeneration of an individual or of all remote area graphics from the removable media used for backup.

g. Contain an editor for user preparation and editing of individual remote area graphics that can be easily generated and that provides a means for easily linking icons to sensors, provides copy and delete functions for entire remote area graphics, can be learned in a two hour period by a person familiar with at least one commercially available graphics software product. The editor shall also provide for producing a standard remote area graphic, making a single character change to an existing graphic, and enabling lines to be easily and accurately aligned and connected.

h. Provide a unique site-specific graphic representation (or scale map) of the complete system, to include all remote areas, RSMs, and the PMC area. The objective of this display is to provide the operator with a geographic perspective representation of remote area alarms with respect to the entire site to aid in assessing the intrusions and dispatching the response force. The PMC shall provide the maintainer the capability to generate a custom

map of the entire site, including the PMC area, RSM areas, all remote areas, buildings, prominent terrain, roads, and any other significant, site unique features. The user shall have the capability to assign defined, unique, and easily identifiable symbols for each remote area, which indicate remote area status using the following color code for the status of the remote areas: (NOTE: Indicators for sensors are not permitted due to the scale of the maps.)

- Steady green indicates SECURE operation (all sensors reset and no alarm and no sensors in ACCESS),
- Steady yellow indicates ACCESS of one or more sensors,
- Flashing red indicates at least one unacknowledged alarm,
- Steady red indicates all alarms acknowledged.

i. Share the remote area graphic display. The operator shall have controls to select either a display of the geographic map or the individual remote area graphics. The first alarm, in an empty alarm queue, shall automatically cause the remote area graphic, in alarm, to be displayed. Subsequent incoming new alarms or status changes shall not cause the display to change until the operator manually selects another display. The graphics shall update within 0.5 seconds after any status change.

3.4.2.1.9 System Data Storage.

The PMC shall use an operating system and have sufficient storage capacity and processing speed to meet the requirements of this performance specification. Hardware and software incorporated in the PMC shall be state-of-the-art programs and devices that can reasonably be expected to be commercially supportable during the next five to seven years. The system shall have the capability to continuously and automatically store system configuration, system status, all operator actions, all periods of maintenance, and all alarm data with corresponding date and time of day into nonvolatile storage. The PMC shall be capable of selectively retrieving and printing the stored data in user-selected formats by date, time

period, and type of data while on-line. The operator shall have no control of data storage. Access to replacing, printing, or backing up the historical data shall be restricted to the appropriate access level of personnel by key lock, password or other control. Provisions shall be available to allow one (1) month storage of archive data before the data must be downloaded to a permanent storage media. The system shall generate a status display message before the capacity of the data storage is reached. The message shall be generated in adequate time to replace the storage media or backup the stored data before overwriting occurs.

3.4.2.1.10 Uninterruptible Power Supply Functional Requirements.

The Uninterruptible Power Supply (UPS) shall:

a. Operate on either of the following nominal voltages and frequencies, depending on available facility power:

(1) 120/208/240 Vac, 60 Hz,

(2) 220 Vac, 50 Hz.

b. Provide converted facility power at the levels required by one PMC during normal operation. The UPS may be an integral part of the PMC or a separate item.

c. Starting with a full charge, provide battery backup capable of supplying power to the PMC during facility power interruptions, for a minimum of eight hours duration, at the lowest specified operating temperature.

d. Automatically switch to backup power, upon loss of primary power, and revert when the power returns without interruption or degradation to the functioning of the PMC.

e. Be sufficiently recharged within twelve hours, after return of normal facility power, to provide power through another eight-hour facility power interruption.

f. Provide discrete output(s) indicating the status of internal tamper switches.

g. Provide discrete output(s) indicating the status (absence or presence) of primary AC power.

h. Monitor the battery voltage. If an overcharging condition at the battery terminals is measured, the primary AC supply and battery charging circuit shall be disabled and the UPS shall operate from the battery. If an under-voltage condition at the battery terminals is measured while operating from the batteries, the positive battery lead shall be opened to prevent excessive discharge. The battery lead shall be automatically reapplied after return of primary AC power. If a DC supply output exceeds or drops below a safe operating level, indicating a DC supply failure, both the primary AC and battery shall be disabled.

i. Be capable of sustaining momentary overloads of 125% of rated voltage for up to 10 minutes, and sustaining surges of 150% of rated capacity for 10 seconds.

j. Provide EMI, transient voltage, and surge protection in accordance with paragraph 3.11 to prevent damage to equipment from lightning and other conducted electrical disturbances or, to localize damage in easily repairable low-cost components.

k. Operate in the interior controlled environment.

l. Be either internal, free-standing, or wall-mountable.

m. Provide the capability to manually switch from primary to battery power as a maintenance function, and to manually bypass the UPS.

3.4.2.1.11 CCTV Interfaces.

The PMC interfaces for the CCTV system are described below. The CCTV characteristics are specified in ICIDS-PS-0701.

a. Interface with a switching matrix controlling groups of 4 cameras up to a total of 128 cameras.

b. The operator interface shall be the CCTV control device, and visual presentations via the TV monitors. Controls for the CCTV system shall be integrated into the operator input device to allow manual operator-triggered, as well as automatic alarm-triggered, camera selection onto any of the four monitors. The alarm-triggered camera selection shall be effective only for the first alarm into the alarm queue; in the case of multiple alarms, the video for subsequent alarms must be manually selected.

c. The PMC system shall interface directly with the CCTV equipment and provide commands to the video switching matrix. The PMC shall process commands, perform data conversions to meet component interfaces, and output commands to CCTV components. The PMC shall output the identification of each alarmed remote area to the CCTV equipment within 3.0 seconds of the sensor alarm in order to make video assessment available to the operator not more than 1.0 second after the alarm is displayed on the PMC.

d. The PMC shall provide the capability, and provide sufficient memory and programmability, for implementation of an automatic mode of operation such that a single alarm at the monitor shall cause a display of up to four camera inputs from the alarmed remote area.

3.4.2.1.12 Physical Characteristics.

All components, subsystems, and subassemblies shall be readily accessible for maintenance. All enclosures shall be lockable. The operator interfaces shall be ergonomically situated for easy access, by the operator, to all controls and displays. The PMC shall be modular to permit ease of assembly, maintenance, and installation. All modules shall be capable of passing through a doorway 81 centimeters wide by 193 centimeters high.

3.4.2.2 Remote Area Data Collector (RADC).

3.4.2.2.1 Description.

RADCs are remote area items that interface sensors, sensor stimuli, response devices, Entry Control Equipment (ECE), CCTV components, and tamper devices with the PMC. Sub-RADCs are remote area items that interface sensors, sensor stimuli, CCTV components, and ECE devices with RADCs. Each RADC shall be capable of interfacing with a minimum of five (5) sub-RADCs. RADCs and sub-RADCs shall be available in various configurations to satisfy the requirements of installations worldwide. Table 1 is a summary of RADC and Sub-RADC requirements.

Table 1: RADC Configurations

RADC TYPE	VOLTAGE	NO. OF SENSORS (1)	ECE I/F (2)	KEYPAD I/F (2)	MODEM (2)	RESP DEVICE I/F (2)&(3)
INTERIOR RADC	12 Vdc	4 min 32 max	YES	YES	YES	YES
INTERIOR SUB-RADC	12 Vdc	4 min 32 max	YES	YES	NO	NO
EXTERIOR RADC	12 Vdc	4 min 32 max	YES	YES	YES	YES
EXTERIOR SUB-RADC	12 Vdc	4 MIN 16 MAX	YES	YES	NO	NO

(1) A minimum of four sensor inputs with capability of additional sensor inputs in increments, up to a maximum of 32 sensor inputs.

(2) “YES” means required. “NO” means not required.

(3) A minimum of four relay outputs or four response device outputs is required. The number of outputs increases in increments, to a maximum of 32 total outputs.

3.4.2.2.1.1 Interior RADCs.

Interior RADCs shall be available to interface with Entry Control Equipment (ECE), keypad, variable numbers and

types of sensors, sensor stimuli, response devices, and CCTV, all individually resolvable. Sub-RADCs need not interface with response devices, but must have relay outputs and be capable of operating with a keypad. Interior RADCs shall be available configured as follows:

a. A minimum of four sensor inputs, with a capability of additional sensor inputs in increments up to a maximum of 32 sensor inputs. Sub-RADC requirements are identical, as shown in Table 1.

b. Ability to communicate directly with the PMC for both high security and regular remote areas. Sub-RADCs need only communicate with RADCs.

c. Sub-RADCs shall have the capability to act as slaves to, and communicate with, other RADCs.

d. A capability to provide +12 VDC to all connected off-the-shelf commercial sensors.

e. A minimum of four relay outputs, or four response device outputs, with a capability of additional relay/response outputs in increments up to 32 total outputs.

3.4.2.2.1.2 Exterior RADCs.

Exterior RADCs shall be available to interface with Entry Control Equipment (ECE), keypad, variable numbers and types of sensors, sensor stimuli, CCTV components, and response devices, all individually resolvable. Sub-RADCs need not interface with response devices, but must have relay outputs. Exterior RADCs shall be available configured as follows:

a. A minimum of four sensor inputs, with a capability of additional sensor inputs in increments up to a maximum of 32 sensor inputs.

b. Capability to communicate directly with the PMC for both high security and regular remote areas. Sub-RADCs need only communicate with RADCs.

c. Sub-RADCs shall have the capability to act as slaves to, and communicate with, other RADCs.

d. Operate in an exterior environment.

e. Four relay outputs, or four response device outputs, with a capability of additional relay/response outputs, in increments up to 32 total outputs.

3.4.2.2.2 PMC Interface.

All RADCs shall communicate all status changes and commands with the PMC, in accordance with paragraph 3.4.2.1.3.

3.4.2.2.3 RSM Interface.

If the system configuration accommodates an interface between the RSM and the RADCs, the data to be exchanged over this interface shall be sufficient to meet the RSM performance requirements of paragraph 3.4.2.3.

3.4.2.2.4 DAS Interface.

All RADCs and sub-RADCs shall interface with a DAS for increased data transmission security, as described in paragraph 3.4.2.5.

3.4.2.2.5 Interior Sensor Interfaces.

All interior RADCs and sub-RADCs shall:

a. Interface with commercial interior sensors (with the sensors being individually resolvable), and interface with response devices. Note: Sub-RADCs need not interface with response devices.

b. Provide an interface to tamper switches associated with the individual sensors.

c. Communicate to the sensors over a minimum distance of 150 meters.

d. Provide power to all connected sensors.

e. Operate over a dedicated hardwired link.

f. Support sensors having relay contacts as an alarm output or solid state equivalents, either normally open or normally closed.

g. Provide a sensor stimulus activation output for each sensor. This output shall be activated by a self-test command from the PMC, RSM, or locally from the RADC maintainer interface. The stimuli activation output shall be a relay or voltage output that shall turn on to activate the sensor stimuli and remain on for a maximum of 8 seconds. This output shall then turn off within one second after the associated sensor alarms. For SCIF areas, the maximum on period shall be limited to 1 second. Salient characteristics for the sensor stimuli are detailed in the individual sensor PES. The RADCs are not required to provide power to the sensor stimuli.

h. Provide supervision of the lines to the sensors to detect tampering, such as shorting or cutting. Current, voltage, impedance monitoring or other effective techniques may be used.

i. Provide EMI, transient voltage, and surge protection on all sensor interface lines, in accordance with paragraph 3.11.

j. When communication is lost between the RADCs and remote area devices (e.g., sensors), a distinct alarm, shall be annunciated at the PMC and/or, the RSM.

3.4.2.2.6 Exterior Sensor Interfaces.

All exterior RADC and sub-RADC sensor interfaces shall be the same as the interior sensor interfaces described in paragraph 3.4.2.2.5, above, with the following exceptions:

a. The minimum operating distance shall be 1000 meters.

b. Need not provide power to the exterior sensors.

c. Sub-RADCs need not interface with response devices.

3.4.2.2.7 Response Device Interface.

All RADCs shall interface to response devices. The response devices shall be triggered (activated) under direct command from the PMC through the RADC. The RADCs shall provide

the capability to enable, disable, activate, and deactivate response devices through PMC operator command. The enable command shall be used to place the response device into a ready state (armed). The disable command shall return the response device to a quiescent state (unarmed). The activate command shall latch the response device on, and shall be effective only if all required conditions cited below are met. The deactivate command shall return the response device to the quiescent state and reset the activate latch. A response device shall not be activated unless all of the following conditions are present: 1) the response device has been previously enabled; 2) the RADC is in the SECURE mode of operation; 3) a valid alarm is active in the same remote area; and 4) the response device activate command has been received. The response device interface shall also:

a. Provide a minimum of four response device channels in the RADCs.

b. In the interior RADCs, communicate to the response devices over a minimum distance of 150 meters.

c. In the exterior RADCs, communicate to the response devices over a minimum distance of 1000 meters.

d. Operate over a dedicated hardwired link (metallic wire or fiber optic cable).

e. Provide a response device status input to support response devices having a normally open or normally closed relay contact output that indicates the ready or spent status of the device.

f. Provide response device enable and activate output relays, either normally open or normally closed contacts (Form C), with a minimum contact rating of 0.25 amperes at 24 Vdc.

g. Support response devices having a tamper switch or relay tamper alarm output, either normally open or normally closed contacts.

h. Provide line supervision to detect line tampering, such as shorting or cutting. Current,

voltage, or impedance monitoring, or other effective techniques may be used.

i. Provide EMI, transient voltage, and surge protection on all response device interface lines, in accordance with paragraph 3.11.

3.4.2.2.8 ECE Interface.

All interior RADCs shall interface as follows:

a. To Entry Control Equipment (ECE), as specified in ICIDS-PS-0702, for receiving and displaying entry control information (e.g., entry approved, entry denied alarms, and tamper information). Upon entry approval, sensor alarms generated during ingress shall be inhibited during a variable (0-90 second) delay. For SCIF applications, the ingress delay shall not exceed 30 seconds. The ingress delay provides an authorized user adequate time to enter the area and switch the RADC from the SECURE to the ACCESS mode of operation.

b. As a user option, when an entry approved message is received from an attached ECE, the RADC status shall be changed from SECURE to ACCESS. The alternate user option is to require the mode change to be performed manually by a key switch or a keypad. This function may be implemented at the RADC or the PMC. The RADC status change shall be displayed, but require no operator action to acknowledge or reset. The RADC identity, status change and time of each ECE event shall be retained in the non-volatile system data storage and the Personal Identification Number (PIN)/badge number and badge holder identification information shall be retained either locally at the ECE or at the PMC.

c. Prohibit the ECE, installed outside the SCIF, from automatically changing the RADC mode of operation to ACCESS, SECURE, OFF-LINE, or from shunting any sensors within the SCIF without continuous annunciation of the shunted sensors at the PMC. Additionally, the identity of ECE users

in SCIFs shall not be divulged to the console operator, except by some coded identifier.

d. PMC interface shall be accomplished either directly to the PMC or through a RADC located in the vicinity of the PMC.

e. Intrusion alarms shall have a higher priority than ECE.

3.4.2.2.9 RADC and Sub-RADC Power Supplies.

All RADC and sub-RADC power supplies shall:

a. Provide the RADC or sub-RADC and all attached sensors with operating power. The minimum load capacity of the power supply shall be 0.25 ampere @ 12 Vdc for eight (8) attached sensors, plus the power requirement of the RADC or sub-RADC. If the RADC sensor capacity is greater than eight (8), then the supply is required to provide a corresponding additional power at a level of approximately 30 milliamperes per sensor.

b. Operate on either of the following nominal voltages and frequencies, depending on available facility power:

(1) 120/208/240 Vac, 60 Hz.
(2) 220 Vac, 50 Hz.

c. Include battery backup, capable of supplying sufficient power to the RADC or sub-RADC and attached interior sensors, during facility power interruptions for a minimum of eight (8) hours at the lowest specified temperature.

d. Automatically switch to backup power, upon loss of primary power, and revert when the primary power returns, without interruption or degradation of the functioning of the RADC or sub-RADC and the connected sensors.

e. The battery shall be sufficiently recharged, within 12 hours after the return of primary power, to provide power through another eight (8) hour primary power interruption.

f. Be located within the RADC or sub-RADC enclosure.

g. Provide discrete output(s) indicating the status (absence or presence) of primary power.

h. Continuously monitor the battery voltage. If an over-voltage condition is measured at the battery terminals, the primary AC supply and battery charging circuit shall be disabled and operation shall continue on the battery. If an under-voltage condition is measured at the battery terminals while operating from the battery, the positive battery lead shall be disconnected to prevent excessive discharge. The battery lead shall be automatically reapplied after return of primary AC power. If a DC supply output out-of-tolerance condition is measured, indicating a power supply failure, both the primary AC and battery shall be disabled. Any power loss shall be reported to the PMC.

i. Be capable of sustaining momentary overloads of 125% of rated capacity for up to 10 minutes, and sustaining surges of 150% of rated capacity for 10 seconds.

j. Include EMI, transient voltage, and surge protection, in accordance with paragraph 3.11, to prevent damage to equipment from lightning and other conducted electrical disturbance, or to localize damage to easily repairable, low-cost components.

k. Operate in either or both interior and exterior environments.

l. Include a capability to manually switch from primary power to battery power as a maintenance function, and to manually bypass the battery.

m. Include an illuminated indication of the power source in use (i.e., AC or DC). The indicator shall change color or flash when operating off the battery.

3.4.2.2.10 RADC/Sub-RADC Maintainer Interface.

All RADCs and sub-RADCs shall provide a means to allow maintenance within the remote area. ON-LINE maintenance shall be utilized unless specific system requirements or safety factors preclude implementation. Maintenance access shall be through a key-locked door. A password or other unique identifier shall be required for access to the maintenance mode. Conduct of maintenance activities shall place the RADCs and sub-RADCs into a maintenance mode, which shall be continuously signaled to the PMC for the duration of the maintenance activity. The RADCs and sub-RADCs shall provide a means to store and display an historical file of the last ten alarms since these devices were last placed into the SECURE mode of operation. A RADC installed in a SCIF shall not have the capability to be remotely diagnosed.

a. All RADCs and sub-RADCs shall have a Built-In Test (BIT) capability to enable maintenance personnel to perform tests of all connected remote area devices. The BIT shall be able to differentiate which connected device(s) are asserting a tamper or communication line failure condition. The BIT shall also provide for fault isolation to the Line Replaceable Unit (LRU).

b. A capability shall also be provided to configure the RADC and sub-RADC address, ingress and egress delay times, and all other configuration actions necessary to properly implement the requirements of these devices. The configuration attributes may be assigned through the maintainer interface or via the PMC, except in the case of SCIFs where remote programming is prohibited.

c. All RADCs and sub-RADCs shall provide a walk-test mode that shall be selectable only while the maintenance mode is active. This mode allows the maintainer to conduct manual walk-tests of the sensors in the remote area. While active, the walk-test mode shall annunciate all sensor and tamper alarms for the duration of the alarm condition and be silent when no alarm is active.

3.4.2.2.11 ACCESS/SECURE Switch/Keypad Interface.

The RADC and sub-RADC shall provide switch/keypad interface as follows:

a. Include an integral, enclosure mounted, key operated, two-position switch for local ACCESS/SECURE mode selection. The RADC and sub-RADC shall monitor this switch for position and report the mode to the PMC. Any mode changes from ACCESS to SECURE shall automatically initiate a self-test of all remote area sensors within 90 seconds after the mode change. It shall not be possible to inhibit tamper or duress alarms in either mode of operation.

b. Provide a capability for bypassing the ACCESS/SECURE switch, thereby removing the capability for local mode changes. With this capability, mode changes shall only be possible when commanded from the PMC or RSM. This capability shall support the implementation of two-person rule at the PMC and/or RSM for ACCESS/SECURE/OFF-LINE mode changes.

c. Provide a keypad as an alternative to the ACCESS/SECURE switch, and accept the output of a keypad or entry control equipment that can uniquely identify an authorized user. When the authorized user enters his unique PIN, or is otherwise uniquely identified (i.e., smart card or biometric device), the RADC or sub-RADC shall automatically change modes from ACCESS to SECURE or SECURE to ACCESS. The user’s identity shall be logged at the PMC or RSM, as applicable. Remote mode changes (e.g., from the PMC or RSM) are expressly prohibited for RADCs used in SCIFs and must be disabled when this mode of operation is selected at initial configuration. Entry control equipment within the SCIF may be used for the mode change, provided that the mode change process is handled entirely within the SCIF and is completely disassociated from normal entry control activities.

d. When in the SECURE mode of operation, the RADC or sub-RADC shall report all sensor and tamper alarms and be capable of enabling, disabling, activating, and deactivating response devices. Video assessment devices shall be capable of

being activated when in the SECURE mode of operation.

e. When operating in the ACCESS mode, all response device activation and sensor alarm annunciation shall be inhibited, except for sensors not ACCESS INHIBITED at installation. Video cameras shall not be capable of being activated when in the ACCESS mode of operation,

f. When the ACCESS INHIBIT mode of sensor operation is implemented at the PMC, RADC or sub-RADC at installation, sensor(s) so configured are inhibited from being ACCESSED. These selected sensors remain in the SECURE mode and all alarms from these sensors shall be reported and displayed, at the PMC and RSM, regardless of the mode of operation.

3.4.2.2.12 Physical Characteristics.

The RADC and sub-RADC enclosures shall have a key-locked door. The enclosure shall be designed to meet the specified environmental conditions. The enclosures shall be metallic and meet the requirements of a NEMA 3R enclosure as specified in NEMA 250. Interior structural components shall have the strength and rigidity to conform to the conditions specified in UL 1076, Section 7. The door and any removable covers shall be provided with door/cover operated corrosion-resistant tamper switches. Enclosure construction shall ensure battery safety. The enclosure shall be capable of being mounted on a horizontal surface, wall, or post.

3.4.2.3 Remote Status Monitor (RSM).

3.4.2.3.1 Description.

The RSM shall be capable of two modes of operation: 1) a display-only mode wherein all, or user selected portions, of the ICIDS status is displayed; and 2) a CCD mode wherein the control of all, or a user selected portion, of the system shall be transferred from the PMC to the RSM. The RSM shall provide an input device to enable the operator to interact with the system when in the CCD mode.

The major functional areas of the RSM are:

a. Command, Control and Display (CCD)

b. Status display

c. Operator interface

d. Interconsole interface (RSM to PMC)

e. Enrollment

3.4.2.3.2 Command, Control and Display Processing.

The RSM shall:

a. Provide two modes of operation, selectable at the user's option:

(1) Command, Control and Display (CCD) Mode. The RSM shall provide a mode (selectable via key switch or password) in which it is capable of assuming command and control of all or part of the connected RADCs from the PMC, and releasing control back to the PMC automatically or upon command. The RSM shall provide the capability, upon configuration at the user's option, to assume control of remote areas assigned to it. In this operating mode, the RSM shall be capable of performing all of the command and control functions of the PMC as specified in paragraph 3.4.2.1.3, except as excluded in paragraph 3.4.2.3.1. A typical application of an RSM, in this mode of operation, would be a facility which assumes control of the remote areas within its perimeter during the working hours of the day, and relinquishes control to the PMC at night.

(2) Display-Only Mode. The RSM shall provide a display-only mode in which the operator has no control over system functions, except to acknowledge or concur with two-person rule requests. In this mode, the RSM shall receive and display all, or user-selected portions, of the system status being displayed at the PMC (e.g., mimic the PMC status display). The RSM shall permit the

operator to monitor the actions of the PMC operator.

b. Monitor all PMC, RSM, and remote area communications and data flow, as the system architecture dictates.

c. Provide the communication interfaces to connected RADCs/sub-RADCs and/or PMCs with the following capabilities:

(1) Send and receive data by one or more of the following separate interfaces and data link subsystems. The choice of data link shall be made prior to installation and shall not limit any system performance nor preclude the use of the DAS. The RSM is required to support any combination of the following data links, selected by the user:

(a) Interfaces with continuous metallic wire pairs. This hardwired link shall be compatible with the DAS, whether internal or external.

(b) A commercial RF/microwave data link may be specified, by the Government, prior to installation for some or all remote areas or PMC-to-RSM data communication. It shall be compatible with the metallic wire pair interfaces at the PMC, RSM, and RADC, and shall also be compatible with the DAS, whether integral or external.

(c) A commercial fiber optic communication interface is an option to be specified, by the Government, prior to installation for some, or all, remote areas or PMC-to-RSM data communication. The transmit/receive circuitry, which interfaces to the fiber cable, may be internal (e.g., replaces hardwired modem) or external (e.g., connects to PMC hardwired output). It shall be compatible with the PMC, RSM and RADC data communication interfaces. The fiber optic communication interface shall utilize fiber optic cable and components as specified in

UFGS 27 21 10.00 10, Fiber Optic Data Transmission Media for Security Systems.

(2) Execute error detection and line supervision processes in order to monitor, detect, and report the loss of line integrity of the communication links.

(3) The RSM-to-PMC and RSM-to-RADC links (as architecture dictates) shall be capable of operating up to 16 kilometers without repeaters or relays, regardless of the type of data link used. This communication interface is required to be supervised, and communication faults annunciated.

(4) Receive system status information including:

(a) Sensor alarms

(b) Sensor tamper

(c) RADC status including ACCESS/SECURE/OFF-LINE mode

(d) RADC tamper

(e) RADC power supply fail alarms

(f) PMC status

(g) Response device status

(h) Remote area configuration

(i) Self-test commands and results

(j) Entry control equipment data (e.g., entry approved/denied). The RSM shall be notified of any shunted sensor.

d. Monitor the tamper conditions for the PMC, RSM and power supply.

e. Monitor AC power status for the RSM.

f. Monitor operator input device data (commands, requests, etc.).

g. Display system configuration data, including date and time of most recent system configuration changes.

h. Provide for orderly shutdown and restart whenever components are replaced, or have lost information, because of power failure or component failure.

i. Provide for automatic nonvolatile data storage for historical data, system configuration data, and system status (e.g., configuration tables, databases, periods of maintenance, sensor shunting). The operator shall have no control of data storage, and access to replacing, or backing up the historical data is restricted to personnel with the appropriate level of access.

j. Have provisions for automatic storage of system configuration data and automatic reinitialization of system configuration from data storage after any system outage (i.e., power outage or system maintenance downtime). Reinitialization time, from power on until full system operation, shall not exceed five minutes.

k. Provide sufficient reserve capacity in main memory to accept future software changes and system expansion. Main memory is memory from which stored programs are executed and within which program data, and input/output operations are stored.

l. Provide for both a manual and an automatic self-testing of the system with the capability for user definable and programmable parameters at installation. These parameters shall include duration of test, number of tests per a given time period. The interval between automatic tests shall be randomized. Intentional alarms generated on a specific device, while under self-test, shall be suppressed. Any valid alarm, such as intrusion, tamper or duress (other than an intentional alarm), generated during a self-test,

shall cause the self-test to terminate and the alarm shall be annunciated. The results of all self-tests shall be recorded in the system data storage. Only self-test failures shall be annunciated at the RSM(s) status displays. Any mode change from ACCESS to SECURE shall automatically initiate a self-test of the remote area equipment within 90 seconds after the mode change.

m. Provide EMI, transient voltage, and surge protection on all external interface lines, in accordance with paragraph 3.11.

n. Provide for two processes to change the ACCESS/SECURE mode of operation of a RADC for an individual sensor or for the entire RADC: 1) from the RSM in CCD mode, or 2) from the RADC. The functional requirements of the ACCESS and SECURE modes are as described for the PMC.

The RSM in the CCD mode shall provide the operator the capability to change the ACCESS/SECURE/OFF-LINE mode of a remote area or sensor by entering a command at the keyboard (except for SCIF areas where remote commanded ACCESS/SECURE/OFF-LINE is prohibited or locked-out at installation). The two-person rule requirements apply to commanded ACCESS/SECURE/OFFLINE mode changes when so configured at installation.

The RSM in both the CCD and Display-Only modes shall monitor and continuously display the mode of operation of the sensors and RADCs. SECURE mode shall be indicated by green color for icons, indicators and graphics. ACCESS shall be indicated by yellow color. Alarms shall be displayed in red.

o. Provide a unique, audible alarm that is activated to alert the operator when any alarm displayed at the PMC remains unacknowledged by the PMC operator for a preset time. The audible alarm is in addition to the visual alarm displayed on the RSM status display. The time limit is adjustable

as a maintenance function and is set at initial RSM configuration.

3.4.2.3.3 Operator Interface.

The RSM operator interface shall provide:

a. An operator input device (e.g., keyboard, mouse, etc.). While the RSM is in CCD mode, the operator input device shall provide all of the functions available to the PMC operator, as previously described. The input device shall provide controls which:

(1) Aid display interpretation

(2) Select alternate display formats

(3) Silence the audible indicator when an alarm is acknowledged

(4) Clear the display of data pertaining to status changes which have been acceptably processed by the console operator

(5) Adjust the auditory signal volume to be heard above any expected ambient noise

While the RSM is in display-only mode, the operator input device and all command and control functions shall be disabled.

b. A maintenance input device, such as a keyboard or other device, to permit a maintenance technician to perform the following maintenance activities. Unauthorized access to the maintenance input device shall be protected against by a mechanical and/or electrical lock (e.g., password, locked panel, etc.). The maintenance tasks shall include:

(1) configuration modifications, both at initial installation and as required, including setting the time and date,

(2) system initialization and reinitialization, which shall be independent of the PMC and its operator,

(3) system self-diagnostics (shall be disabled for RADCs installed in SCIFs), and

(4) selecting the portion of the PMC display to be displayed at RSM (if accomplished at RSM).

c. A status display. Shall utilize a visual display, in color, of at least 48 centimeters diagonal in size with a minimum resolution of 1280 by 1025 pixels. While the RSM is in CCD mode, the status display shall function as described herein for the PMC.

While the RSM is in display-only mode, the status display shall:

(1) display all, or selected portions, of the host PMC system status, independent of the PMC (i.e., the RSM operator may autonomously select any display, regardless of the display currently selected at the PMC),

(2) reject status data explicitly disabled during RSM initialization or configuration, and

(3) display data in a format similar to the PMC status display; this shall include video and audible indicators. However, the format shall be modified such that the RSM operator can monitor keyboard responses by the PMC operator.

3.4.2.3.4 Interconsole Interface.

The RSM shall:

a. Communicate (directly, if architecture dictates) with the PMC to receive all, or selected portions, of the system status and all PMC

operator actions for use by the RSM (depending on operating mode).

b. Interface with a DAS to encrypt system data for use by the RSMs. Disruption or loss of these communication lines shall be annunciated at the PMC and RSMs as line security alarms.

3.4.2.3.5 Uninterruptible Power Supply.

The RSM UPS shall perform in accordance with the requirements for the PMC UPS described in paragraph 3.4.2.1.10.

3.4.2.3.6 System Data Storage.

The RSM shall use an operating system and have sufficient storage capacity and processing speed to meet the requirements of this performance specification. Hardware and software incorporated in the RSM shall be state-of-the-art programs and devices that can reasonably be expected to be commercially supportable during the next five to seven years. The system shall have the capability to continuously and automatically store system configuration, system status, all operator actions, all periods of maintenance, and all alarm data with corresponding date and time of day into nonvolatile storage. The RSM shall be capable of selectively retrieving and printing the stored data, in user selected formats, by date, time period, and type of data, while on-line. The operator shall have no control of data storage, and access to replacing, printing, or backing up the historical data shall be restricted to the appropriate access level of personnel by key lock, password or other control. Provisions shall be available to allow a one (1) month storage of archive data before the data must be downloaded to a permanent storage media. The system shall generate a status display message before the capacity of the data storage is reached. The message shall be generated in adequate time to replace the storage media or backup the stored data before overwriting occurs.

3.4.2.3.7 Physical Characteristics.

The RSM shall be modular to permit ease of assembly, maintenance, and installation. All modules shall be capable of passing through a doorway 81.25 centimeters wide by 193 centimeters high. The RSM and UPS shall both be free-standing, floor-mounted. The UPS shall also be capable of being mounted, remotely, up to 15.25 meters from the RSM.

3.4.2.3.8 Closed-Circuit Television (CCTV) System Interface.

The RSM does not require an interface with the CCTV.

3.5 Data Authentication System (DAS).

3.5.1 Description.

The Data Authentication System (DAS) shall provide secure data communication using National Institute of Standards and Technology (NIST) validated Data Encryption Standard (DES) encryption or Advanced Encryption Standard (AES) as specified in FIPS-197 and conforming to the requirements of FIPS-140-2, for data communications between PMC-to-RSM, PMC-to-RADC, and RSM-to-RADC (if architecture dictates). The DAS may be internal or external, and may be optionally installed within the PMC, RSM, and RADC enclosures. In either case, the DAS shall be physically compatible and electrically interoperable with the PMC, RSM and RADC hardwired data links, and other system components, including the optional fiber optic communication interface, and the optional RF/microwave data link. It shall derive operating power from existing power source(s). The DAS shall provide the capability to remotely install or change the RADC encryption key.

3.5.2 DAS Interfaces.

The Data Authentication System (DAS) interfaces shall consist of external interfaces defined in the following paragraphs:

a. DAS communication interfaces. The DAS shall provide optional data encryption capability for applicable PMC, RSM, and RADC communication channels whether hardwired, RF/microwave, or fiber optic. The DAS equipment shall receive an encryption key variable from a key carrier, in the case of local keying, or from the host console or remote keying device, in the case of remote keying capability.

b. DAS electrical interfaces. The DAS shall derive electrical power from the PMC, RSM, or RADC, as applicable. Power consumption shall be compatible with host component requirements for power consumption, backup power capability, and thermal design. The DAS shall provide an

interface(s) compatible with the hardwired, RF/microwave and fiber optic data links.

c. DAS physical interfaces. The DAS components shall be modular to allow for optional installation within the PMC, RSM, or RADC for site specific applications. The DAS components commonality in design and form factor shall be maximized in the interest of interchangeability and inventory cost reduction. The form factor and weight of DAS components shall be consistent with specified modularity and redundancy requirements and with space limitations within the PMC, RSM, and RADC enclosures. Each DAS unit shall be of modular form to allow configuration for either encrypted or non-encrypted operation.

3.5.3 DAS Functional Characteristics.

The DAS shall provide data encryption for the specified communication channels. A DAS secure communication channel will require installation of a DAS device at each end of the communication link (e.g., within the PMC and within the RADC). The DAS shall provide sufficient capacity, flexibility and redundancy to allow any or all eligible communication channels of a PMC, RSM, or RADC to operate simultaneously in the encryption mode.

3.6 Radio Frequency (RF)/Microwave Communication Network

3.6.1 Description.

The RF/Microwave communication network shall be an option for the PMC, RSM, and RADC in place of any or all of the metallic wire pairs (hardwired lines).

3.6.2 Interface Requirements.

The RF/Microwave communication network shall provide the same interface specified for metallic wire pairs and be installed in place of the hardwired communication link at the user's determination.

3.6.3 Functional Requirements.

The RF/microwave communication network shall function under the PMC, RADC, and RSM program control and conform to the specified functional requirements for metallic wire pairs.

3.7 Fiber Optic Communication Interface.

3.7.1 Description.

The fiber optic communication interface shall be a user option for interfacing the PMC, RSM, and RADC in place of any or all of the metallic wire pairs (hardwired lines).

3.7.2 Interface Requirements.

The fiber optic communication interface shall provide the same interfaces specified for metallic wire pairs, described herein.

3.7.3 Functional Requirements.

The fiber optic communication interface shall function under the PMC, RADC, and RSM program control and conform to the specified functional requirements for metallic wire pairs, described herein. The PMC, RSMs and RADCs shall provide all necessary data communication circuitry to interface to fiber optic cable and components, per guidance contained in UFGS 27 21 10.00 10.

3.8 Human Factors Engineering (HFE).

To facilitate ICIDS performance, Human Factors Engineering (HFE) shall ensure that detected events are easily recognized by the operator. Displays that alert the operator to events requiring a response shall be clear and complete. The HFE principles and design requirements of commercial standards shall be used as guidance to ensure the effectiveness of man-equipment interfaces (e.g., controls, indicators, and displays) and to eliminate unnecessary demands on human skill, training, and manpower.

3.9 Safety.

a. To the maximum extent possible, the components shall be composed of such materials and operate in such a fashion that neither its presence nor operation shall impair the health or safety of persons coming near or into contact with it.

b. The design shall incorporate positive methods to protect operating and maintenance personnel from accidental contact with hazards. No special clothing, training, or equipment shall be

necessary for safe operation of the remote area items.

c. Special handling requirements and other safety precautions shall be conspicuously labeled. All equipment shall meet the requirements of National Electrical Code (NFPA-70 2005), Life Safety Code (NFPA-101 2006), and shall be in accordance with applicable UL 1076 safety standards as guidance to ensure ICIDS is safe to operate and maintain.

3.10 Environmental Requirements.

3.10.1 Natural Environment.

The components of the CCDS shall withstand environmental conditions, or combinations of, as follows:

3.10.1.1 Interior Components

3.10.1.1.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -10^{o} C and +60^{o} C.

3.10.1.1.2 Operating Conditions.

a. Temperature.

(1) For console area components, shall be able to operate, as specified herein, in any temperature between +10^{o} C and +40^{o} C.

(2) For other interior area components, shall be able to operate, as specified herein, in any temperature between 0^{o} C and +50^{o} C.

b. Relative Humidity. The CCDS components shall be able to operate, as specified herein, in any relative humidity between 20% and 85% (non-condensing).

3.10.1.2 Exterior Components

3.10.1.2.1 Non-Operating Conditions.

Shall not be damaged in any temperature between -10^{o}C and +60^{o}C.

3.10.1.2.2 Operating Conditions

a. Temperature. The CCDS components shall be able to operate, as specified herein, in temperatures between -10^{o} C and +50^{o} C.

b. Relative Humidity. The CCDS components shall be able to withstand relative humidity between 20% and 85% (non-condensing).

c. Rain. The CCDS exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 57.

d. Dust. The CCDS exterior components shall not be damaged and shall operate, as specified herein, when tested for one hour as specified in UL 639, Section 58.

3.10.2 Impact and Vibration.

The CCDS components shall not be damaged and shall operate, as specified herein, when subjected to the jarring test as specified in UL 1076 section 39.

3.10.3 Vibration.

The CCDS RADCs shall not be damaged by vibration when tested, as specified in UL 639, Section 37.

3.11 Electromagnetic Interference (EMI) Control.

3.11.1 Electromagnetic Radiation.

The CCDS shall comply with the requirements of Federal Communications Commission (FCC) Part 15, Class B equipment.

3.11.2 Induced Environment.

The CCDS shall meet lightning, EMI transient voltage and power surge requirements of UL 1076, Sections 44 and 45.

3.11.3 Lightning.

Equipment shall be protected to prevent equipment damage as a result of transient voltage conducted into the equipment through power, communication, and/or control lines by

natural phenomena such as lightning, or to localize damage in easily repairable low-cost components.

3.12 Finish.

3.12.1 Treatment and Painting.

Unless otherwise specified, the portions of the components subject to corrosion shall be cleaned, treated and painted.

3.13 Identification Plate or P/N Marking.

All components of the CCDS shall be identified with make, model/part number and serial number in accordance with UL 1076.

3.14 Workmanship.

Workmanship shall be in accordance with best commercial standards and practices as specified in UL 1076. These requirements are applicable to wiring, welding, brazing, plating, riveting, finishes, machine operations, screw assemblies, and freedom of parts from burrs, sharp edges, or any other damage or defect that could make the part (or equipment) unsuitable for the purpose intended.

4. VERIFICATION.

Verification is the process of inspection to show that the CCDS functions within the ICIDS and meets the requirements of the Performance Specification. All inspection results shall be documented in contractor prepared reports. The Government reserves the right to perform any of the inspections set forth in this specification where such inspections are deemed necessary to ensure supplies and services conform to the prescribed requirements.

4.1 Methods of Verification.

Table 2 provides the methods utilized to accomplish verification including:

a. Contractor performed analysis (C/A) is an element of verification that utilizes established technical or mathematical models or simulations, algorithms, charts, graphs, circuit diagrams, or other scientific principles or procedures to

provide evidence that the stated requirements were met. An "x" in the C/A column of Table 2 indicates that details of the analysis performed by the Contractor shall be provided in the Test Plan and the analysis shall be included in the Test Report.

b. Contractor performed examination (C/E) is an element of verification and inspection consisting of investigation, without the use of special laboratory appliances or procedures, of items to determine conformance to specified requirements. Examination is generally nondestructive and typically includes the use of simple physical manipulation, mechanical and electrical gauging and measurement. An "x" in the C/E column of Table 2 indicates that the Contractor conducted examination shall be included in the Test Plan, and the results of the examination shall be included in the Test Report.

c. Contractor performed test (C/T) is an element of verification and inspection which generally denotes the determination, by technical means, of the properties or elements of items, including functional operation, and involves the application of established scientific principles and procedures. An "x" in the C/T Column of Table 2 indicates that the Contractor conducted test shall be included in the Test Plan. Details shall be provided in the Test Procedure, and the results of the tests shall be included in the Test Report.

4.2 Performance Verification Test (PVT).

Performance Verification Test includes:

4.2.1 Performance Verification Test – 1

Performance Verification Test – 1 includes analysis, examination, and PVT-1 of the fully integrated ICIDS-IV system consisting of at least one component of each hardware/software item. The Contractor shall conduct the test, in accordance with (IAW) Government approved test plans and procedures and using the test methods

described in Table 2, to verify the ICIDS system performance.

4.2.2 Installed Performance Verification Test – 2

Performance Verification Test – 2 includes analysis, examination, and PVT-2 of the first installed ICIDS-IV system to verify performance prior to Government acceptance. Contractor generated, Government approved test plans and test procedures shall be utilized using the test methods described in Table 2 to verify acceptable system performance.

4.2.3 Installed System Acceptance Test

Installed System Acceptance Test includes analysis, examination, and System Acceptance Test (SAT) of each installed ICIDS-IV system, subsequent to the first system, to verify performance prior to Government acceptance. Contractor generated, Government approved test plans and procedures shall be utilized using the test methods described in Table 2 to verify acceptable system performance.

TABLE 2 : Methods to Accomplish Verification

Paragraph		C/A	C/E	C/T
3.4.1.1	To report.			x
3.4.1.2	To assess.			x
3.4.1.3	To deter.			x
3.4.1.4	System timing.			x
3.4.1.5	Tamper protection.			x
3.4.1.6	Printer	x		
3.4.2.1	Primary monitor console.			x
3.4.2.1.1	Description.		x	
3.4.2.1.2	Functional areas.			x
3.4.2.1.3	CCD Functions.			x
3.4.2.1.4	Operator interface.			x
3.4.2.1.5	Remote area communication.			x

Paragraph		C/A	C/E	C/T
3.4.2.1.6	Interconsole communication.			x
3.4.2.1.7	Status display.			x
3.4.2.1.8	Geographic map display.			x
3.4.2.1.9	System data storage.	x		
3.4.2.1.10	UPS.			x
3.4.2.1.11	CCTV interface.			x
3.4.2.1.12	Physical Characteristics.		x	
3.4.2.2.1	RADC Description.			x
3.4.2.2.2	PMC interface.			x
3.4.2.2.3	RSM interface.			x
3.4.2.2.4	DAS interface.			x
3.4.2.2.5	Interior sensor interface.			x
3.4.2.2.6	Exterior sensor interface.			x
3.4.2.2.7	Response device interface.			x
3.4.2.2.8	ECE interface.			x
3.4.2.2.9	RADC/Sub-RADC Power Supplies			x
3.4.2.2.10	RADC/Sub-RADC maintainer interface.			x
3.4.2.2.11	ACCESS/SECURE Switch/Keypad interface.			x
3.4.2.2.12	Physical Characteristics.		x	
3.4.2.3.1	RSM Description.			x
3.4.2.3.2	RSM CCD processing.			x
3.4.2.3.3	RSM operator interface.			x
3.4.2.3.4	Interconsole interface.			x
3.4.2.3.5	RSM UPS.			x
3.4.2.3.6	RSM system data storage.	x		

Paragraph	C/A	C/E	C/T
3.4.2.3.7 RSM physical characteristics.		x	
3.5.1 DAS functions.			x
3.5.2 DAS interface.			x
3.5.3 DAS functional characteristics			x
3.6.1 RF/Microwave comm.	x		
3.6.2 RF/Microwave interface.	x		
3.6.3 RF/Microwave functions.	x		
3.7.1 Fiber optic communication	x		
3.7.2 Fiber optic interface.	x		
3.7.3 Fiber optic functions.			x
3.8 HFE.		x	
3.9 Safety.		x	
3.10 Environmental Requirements	x		
3.11 EMI Control.	x		
3.12 Finish.		x	
3.13 Id Plate Or P/N Marking.		x	
3.14 Workmanship.		x	

5. PACKAGING.

Packing requirements will be specified in Section D of the contract.

6. NOTES.

This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.

6.1 Intended Use.

The PMC, RADC, RSM and communication links, specified herein, are components of the ICIDS. The ICIDS will provide intrusion detection capability for DoD resources worldwide.

6.2 Definitions.

Access Control - Access Control ensures that resources are only granted to those users who are entitled to them.

Biometrics - Biometrics use physical characteristics of the users to determine access.

Biometric Identifier - A set of biological characteristics that are unique to an individual and may be used to positively identify a person. Examples of biometric identifiers are fingerprints, facial characteristics, iris pattern, and hand geometry.

Biometric Input Device – An input device which senses the biometric parameters being used as an identifier. Examples are a fingerprint pad, an iris scanner, a hand geometry sensing plate, and other biometric sensors. The input sensor may have processing circuits and associated electronics included within its enclosure (housing). It may operate in a stand alone mode directly communicating with the local processor or it may be operated in conjunction with other devices such as a card reader or keypad and communicate with a remotely located database.

Boundary Penetration Sensors - Sensors that detect penetration through perimeter barriers, such as walls, ceilings, duct openings, doors and windows and include balanced magnetic switches, glass break sensors, grid wire sensors, passive ultrasonic sensors and vibration sensors.

Capacity Proximity Detectors - A sensor designed to detect when an intruder approaches or touches a protected item within a protected area.

Class B Line Supervision - Class B line supervision is based on pseudo random generated tones or digital encoding using an interrogation and response scheme throughout the system. The signal shall not repeat itself within a minimum six month period.

Closed Circuit Television (CCTV) – A properly integrated CCTV assessment system provides a rapid and cost-effective method for determining the cause of intrusion alarms and a cost-effective supplement to guard patrols
Damage – A deformation, corrosion, loosening of parts, breakage, change of fit of any part, physical change which impairs the mechanical integrity of the component, evidence of delamination or water penetration into integrated circuits, printed circuit

boards or parts resulting in non-conformance of a component to the provisions of the performance specification.

Data Authentication System (DAS) - Provides secure data communications using NIST validated Advanced Encryption Standard (AES) as specified in FIPS-197 and conforming to the requirements of FIPS-PUB-140-2, for data communications between the PMC-to-RSM, PMC-to-RADC, and RSM-to-RADC (if architecture dictates). The DAS may be internal or external, and may be optionally installed within the PMC, RSM, and RADC enclosures (called housing by some vendors). The DAS shall be physically compatible and electrically interoperable with the PMC, RSM and RADC hardwired data links, and other system components, including the optional fiber optic communication interface, and the optional RF/microwave data link. It shall derive operating power from existing power source(s). The DAS shall provide the capability to remotely install or change the RADC encryption key. The DAS shall provide data encryption for the specified communication channels. A DAS secure communication channel will require installation of a DAS device at each end of the communication link (e.g., within the PMC and within the RADC). The DAS shall provide sufficient capacity, flexibility and redundancy to allow any or all eligible communication channels of a PMC, RSM, or RADC to operate simultaneously in the encryption mode.

Data Authentication/Class ‘A’ Line Supervision - Encryption of IDS data through the use of an algorithm based on the Advanced Encryption Standard (AES), which complies with FIPS 197, for the purpose of ensuring the integrity and validity of transmitted data.

Duress Sensor - A switch designed to be incorporated into an IDS to provide individuals, located within a protected area, a means of signaling, in a covert manner, that they have been placed under duress. A duress sensor should never be annunciated by a local audible alarm.

Electromagnetic Interference (EMI) - Disruption of the alarm signal caused by electromagnetic disturbance. This can be caused by lightning, power line noise and other electrical devices.

Environmental Alarm - An environmental alarm is the result of sensor activation caused by natural causes such as wind, lightning or thunder.

Failure - Failure of the components listed in 3.2.1 is defined as any relevant malfunction that results in loss of the ability of the equipment to perform its intended function as described in Section 3. Where functional redundancy exists, failure is defined as total loss of that function.

False Alarm - A false alarm is the result of sensor activation for no apparent reason.

False Alarm Rate - The number of alarms produced by unknown sources during a given period of time.

False Rejects - False Rejects are when an authentication system fails to recognize a valid user.

Interior Sensor - Sensors that perform one of three detection functions: detection of an intruder penetrating the boundary of a protected area, detection of an intruder’s motion within a protected area, and detection of an intruder touching or lifting an asset within a protected area.

Intrusion Alarm - An intrusion alarm is the result of sensor activation caused by an actual intrusion or an attempted intrusion into a protected area.

Line Replaceable Unit (LRU) - The LRU is defined as the lowest level component that is normally replaced at the installation level. An example of an LRU might be a printed circuit board rather than a chip or other component mounted on a printed circuit board.

Maintenance Ratio (MR) - MR is defined as the ratio of unscheduled maintenance man hours per operating hour; it includes all unscheduled maintenance actions, repair or replacement, required to keep the CCDS operational. The MR for the CCDS components shall not exceed the values shown below.

Motion Sensor - Sensors designed to detect intruder motion within a protected area. The sensors may be active or passive and include Ultrasonic Motion Sensors, Interior Microwave, and Passive Infrared Motion Sensors.

Nuisance Alarm - A nuisance alarm is the result of sensor activation caused by accident, neglect, natural forces (to include animals), or malfunction of the sensor.

Nuisance Alarm Rate - The number of alarms produced by known, nonhuman causes during a given period of time.

Open System Architecture - A term used to describe any computer or peripheral design that has a published specification. A published specification lets third parties develop add-on hardware for an open architecture computer or device. The term also can refer to a design that provides for expansion slots on the motherboard, allowing the addition of boards to enhance or customize a system.

Probability of Detection (Pd) - The probability that the IDS will detect a human intruder.

Primary Monitoring Console (PMC) – The PMC is defined as the control center that monitors intrusion detection devices for ICIDS. The PMC employs color monitors, operator workstations, a communications cabinet and an uninterruptible power supply (UPS) as a backup power source. The PMC uses an interrogate-response polling sequence to provide the primary command and control for the secure areas also referred to as remote areas. The PMC shall have the capability to monitor up to a minimum of 512 remote areas controlled by RADCs.

Performance Verification Test-1 - Performance Verification Test–1 includes analysis, examination, and PVT-1 of the fully integrated ICIDS-III system consisting of at least one component of each hardware/software item. The Contractor shall conduct the test, in accordance with (IAW) Government approved test plans and procedures and using the test methods described in Table 2, to verify the ICIDS system performance.

Installed Performance Verification Test – 2 - Performance Verification Test – 2 includes analysis, examination, and PVT-2 of the first installed ICIDS-III system to verify performance prior to Government acceptance. Contractor generated, Government approved test plans and test procedures shall be utilized using the test methods described in Table 2 to verify acceptable system performance.

System Performance Verification Test (SPV) – The SPV includes an analysis, examination, and System Acceptance Test (SAT) of each installed ICIDS-III system, subsequent to the first system, to verify performance prior to Government acceptance. The SPV is generated by the Contractor using Government approved test plans and procedures employing test methods to verify acceptable system performance.

Protected Area - The area that contains property or material that is protected by the IDS. Depending on the location/area you are in and what type of IDS you are working with, it can also be referred to as Remote Area(s) or Zone(s).

Radio Frequency Interference (RFI) - Electromagnetic Interference in the radio frequency range, which are frequencies above 100 kHz.

Remote Area Data Collector (RADC) - RADCs are remote area items that interface sensors, sensor stimuli, response devices, Entry Control Equipment (ECE), CCTV components, and tamper devices with the PMC. Sub-RADCs are remote area items that interface sensors, sensor stimuli, CCTV components, and ECE devices with RADCs. Each RADC shall be capable of interfacing with a minimum of five (5) sub-RADCs. RADCs and sub-RADCs shall be available in various configurations to satisfy the requirements of installations worldwide. Table 1 is a summary of RADC and Sub-RADC requirements.

Remote Status Monitor (RSM) - The RSM is typically used by the System Administrator for administrative reports and management of a security zone. Some security zones may also use the RSM to remotely monitor their alarms. An optional configuration provides a backup Server/RSM Workstation CPU in event the PMC malfunctions.

Smart Card – A smart card is an identification credential that contains special information of an individual nature such as digital certificates, digital signatures, and/or biometric identifiers.

Tamper Alarm - An alarm generated by physically interrupting or electrically disrupting communications between the RADC and sensor, or by physically attempting to access the interior of any ICIDS component.

Threat - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Threat Assessment - A threat assessment is the identification of types of threats that an organization might be exposed to.

Threat Model - A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

Threat Vector - The method a threat uses to get to the target.

Uninterrupted Power Supply (UPS) – The UPS provides “true” computer grade power upon loss of line AC for up to eight hours. A UPS microprocessor determines which system mode it should operate in, depending on line conditions but may also be operated manually through the control panel.